September 23, 2016

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: *Notice of ex parte meetings from Audience Partners, LLC*
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

Pursuant to Section 1.1206 of the Commission's rules,[1] Audience Partners, LLC (Audience Partners) provides notice of ex parte meetings on September 21, 2016. Jeff Dittus (CEO and Chairman of Audience Partners), Linda Montemayor (General Counsel and Chief Privacy Officer for Audience Partners), Jo-Ellyn Sakowitz Klein and the undersigned (both as counsel for Audience Partners), met separately with Travis Litman, Claude Aiken, Amy Bender, Nicholas Degani, and Stephanie Wiener to discuss Audience Partners' comments and reply comments that were filed in response to the above captioned proceeding.[2]

Audience Partners' primary concern is ensuring that the Commission's Rule is clearly flexible enough to preserve innovative, privacy-by-design marketing solutions designed to strike a balance between consumer privacy and business interests. Audience Partners explained that its digital advertising company was founded in 2008 by a group of engineers who were concerned about the invasiveness of advertising platforms that relied on tracking, deep packet inspection, and other similar techniques to target advertising campaigns. They believed advertising could be done without compromising consumer privacy. The resulting technology pioneered by Audience Partners is a privacy-by-design platform that uses minimal non-sensitive information to allow ads to be served to desired audiences. The attached slide, which details the Audience Partners process, was provided to Commission staff.

As Audience Partners explained, its doubleblind privacy® technology uses only household street address and IP address as part of a match process that takes place completely behind the BIAS provider's firewall. The system does not collect or use any timestamp or other identifying information, and it even strips out household street address, delivering only a routing table of anonymous IP addresses to be used to serve ads. It does not use browsing history or track consumer location, and it aggregates IP addresses to ensure there are no "lists of one." Moreover, as Audience Partners further explained, its technology recognizes and honors persistent opt-out flags that BIAS providers associate with customer accounts at the household level and ensures that all flagged IP addresses are excluded from any current or future matched lists (and are also deleted from any previously matched lists still in the system). Audience

[1] 47 C.F.R. § 1.1206.
[2] *See* Audience Partners comments, WC Docket No. 16-106 (May 27, 2016) and Audience Partners reply comments, WC Docket No. 160-106 (July 7, 2016).

Partners emphasized that their privacy-sensitive solution ensures that any opt-out exercised will remain effective across all devices accessing the Internet through that IP address.

1. IP Addresses – Particularly Non-Static IP Addresses – Should Be Excluded from the Definition of "PII" in the Rule

Audience Partners expressed that a key element of developing a privacy regime that promotes privacy-by-design technologies such as Audience Partners' is to ensure that the list of data elements that constitute PII is developed, consistent with the Commission's authority under section 222, to include only information that is linked or reasonably-linkable to an individual—and should therefore not include customer IP addresses which are not typically static and are not linkable to an individual.[3] In the *BIAS Privacy NPRM*, the Commission proposes that "information is linked or linkable to an individual if it can be used on its own, in context, or in combination to identify an individual or to logically associate with other information about a specific individual."[4] As Audience Partners explained in its comments and in the meetings, IP address alone is insufficient for identifying an individual, and as noted in its reply comments, a number of parties agree.[5] A dynamic IP address points to a particular device – such as a router in an apartment building or retail establishment – at a particular point in time, and especially without a time-stamp, it is not reasonably linkable to an individual. Moreover, IP addresses are public information,[6] and as Audience Partners and others have noted, it would be unreasonable for the Commission to treat information regularly provided to website operators as PII when that information does not identify an individual.[7]

The construction of the Commission's proposed test for what is linked or reasonably linkable, which includes the conjunction "or," means that IP address would have to be treated as PII, regardless of whether IP address alone is sufficient to be linked or reasonably linkable to an individual. Audience Partners explained in the meetings that there is precedent in other privacy and data protection regimes – including the breach notification laws of many states, which require disclosure of an individual's name together with another identifier for the statute to be triggered – for the stance that certain elements of information on their own are insufficient to

---

[3] Audience Partners noted that customer IP addresses are generally dynamic, and many BIAS providers are moving towards changing IP addresses even more frequently than is presently the case. Audience Partners also explained that even static IP addresses alone do not identify an individual. At a minimum, IP addresses that are not static, not unique, and not persistent should not be PII for purposes of the proceeding.

[4] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Notice of Proposed Rulemaking, 31 FCC Rcd. 2500, 2520 para. 62 (rel. Apr. 1, 2016) (*BIAS Privacy NPRM*) (internal quotations omitted).

[5] *See* Audience Partners comments at 11 ("IP address blocks and individual device IP addresses are necessarily collected and used for the basic functioning of the Internet and that unlike a Social Security Number, mother's maiden name, or even an account user name, the IP address identifies a device (generally a router)—not the individual—and is essential to the functioning of the Internet."); *id*. at 12 ("The National Institute of Standards and Technology ("NIST") guidance on PII, which the NPRM cites as a source that informed the Commission's thinking, makes this point as well, noting in an example that '[t]he user's IP address . . . [b]y itself, [is not] directly identifiable data.'"); *id*. ("Even a static IP address, without being linked to other information, does not identify an individual."); Audience Partners reply comments at 2-4.

[6] An example of publicly-available IP addresses is available at https://iplocation.info/groups/na/us/va/f087cc/.

[7] Audience Partners reply comments at 3.

identify an individual and trigger protections.[8] For these reasons, Audience Partners encouraged the Commission staff to consider a more nuanced approach that would recognize that IP address alone is insufficient to identify an individual and should be excluded from PII unless combined with other information (such as name) that allows the identification of an individual.[9]

2. The Rule Should Provide a Reasonable Opt-Out Consent Regime to Ensure Privacy-Sensitive Practices Can Continue

In response to questions from Commission staff on whether a broader opt-out regime would address Audience Partners' concerns regarding the inclusion of IP address as PII, Audience Partners agreed that depending on the details of such a regime, such an approach could help address their concerns because, as explained above, Audience Partners' privacy-sensitive solution was designed to include a persistent opt-out that is implemented at the household level, so regardless of device or browser used, the consumer's desire to be excluded from Audience Partners' advertising service is ubiquitously respected.

While the *BIAS Privacy NPRM* proposes as its default an opt-in regime and only allows opt-out consent in very limited circumstances, Audience Partners would support efforts to develop a broader opt-out framework that is more focused on the sensitivity of the information collected to determine whether opt-out or opt-in consent is the more appropriate form.[10] We note that the staff of the Bureau of Consumer Protection of the Federal Trade Commission supports such an approach.[11] Audience Partners would suggest that the Commission could narrow its list of what it would consider PII and eliminate non-sensitive information. Alternatively, the various categories of PII suggested in the *BIAS Privacy NPRM* could be grouped into two categories of sensitive information (e.g. medical and health information, financial information and government issued identification numbers) and non-sensitive information (e.g., phone book information such as name and street address, IP address and other non-persistent identifiers), requiring opt-in consent only for sensitive information or when non-sensitive is combined with sensitive information.

Audience Partners is willing to explore such a framework with the Commission to help craft a meaningful mechanism that provides consumers protection for sensitive information, while still allowing commerce to advance through privacy-focused solutions.

3. The Statutory Aggregate Customer Information Exception Should Clearly Apply to Preserve Privacy-Sensitive Data Practices Like Those Employed by Audience Partners.

---

[8] *See* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (compilation of state breach notification laws).

[9] Audience Partners reiterated that this approach is consistent with other privacy regimes, noting that state breach notification laws typically protect data sets that contain name *together with* other data deemed sensitive, such as Social Security Number or driver's license number, or financial account number *together with* relevant passwords or PINs. *See* National Conference of State Legislatures, *Security Breach Notification Laws* (Jan. 2016), available at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[10] *Id*. at 2543-44, paras. 122-126.

[11] Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106, at 9, 23 (May 27, 2016).

With regard to the statutory exception for aggregate customer information, Audience Partners expressed general support for the four-pronged framework set out by the Commission, with a few modifications to ensure it remains consistent with the statute, strikes the proper balance between privacy and commerce, and does not create undue ambiguity for companies like Audience Partners that have designed and implemented privacy-sensitive solutions. Specifically, Audience Partners explained that, unlike the Federal Trade Commission's broad statutory authority, the Federal Communications Commission's relevant statutory definition is focused on "*individual customer identities* and characteristics."[12]

As such, a requirement that BIAS providers determine that the aggregated customer PI is not reasonably linkable to a *device*, as the Commission's explanatory text in the NPRM states in describing the first prong of the standard,[13] is inconsistent with section 222.[14] Audience Partners further noted that, unlike the explanatory text of the NPRM, the draft proposed rule gets this correct, allowing the BIAS provider to use, disclose, and permit access to "aggregated customer PI [that] is not reasonably linkable to a specific *individual*."[15] Audience Partners urged clarification by the Commission that the Rule is limited to linkability to specific individuals, does not encompass linkability to devices, and is therefore, consistent with the statutory limits.

Audience Partners emphasized the importance of retaining the plain meaning and reasonable application of the term "aggregate customer information" from the statute, permitting use and disclosure of a conglomeration of data elements – like IP addresses – that are not reasonably linkable to individuals. Audience Partners noted that its comments referenced standard definitions of the terms "aggregate" and "collective" to demonstrate that those terms do not mean that all individual data elements must be eliminated.[16] In fact, both definitions contemplate retention of individual elements, and Audience Partners urged that the Commission's policy should as well. Further, a more meaningful measure to protect privacy, rather than attempt to focus on linkability to devices, may be to impose a minimum audience size—a step Audience Partners already takes via the requirement that each aggregate routing table developed by its system contains at least 1000 IP addresses, as was explained in the meetings.

With regard to the second prong of the customer aggregate information standard proposed by the Commission, which would require a public commitment to maintain and use the aggregate customer PI in a non-individually identifiable fashion, Audience Partners asked that the Commission make clear in its Order that this prong can be satisfied through inclusion of such assurances in the BIAS provider's privacy policy, which as Audience Partners referenced in its comments, the Federal Trade Commission has noted "provides an important accountability function."[17]

On the third and fourth prongs of the standard, which would require each BIAS provider to "[c]ontractually prohibit[] any entity to which it discloses or permits access to the aggregate consumer PI from attempting to re-identify such information" and to "exercise[] reasonable

---

[12] 47 U.S.C. § 222(h)(2).
[13] *BIAS Privacy NPRM* at para. 154.
[14] *See* Audience Partners comments at 14-15; *see also* NCTA reply comments at 23-24.
[15] *Compare BIAS Privacy NPRM* at para. 154 *with id.*, App. A at 108.
[16] Audience Partners comments at 19-20.
[17] Audience Partners comments at 18.

monitoring" to ensure these contractual obligations are not violated, Audience Partners explained to Commission staff that its contracts with BIAS providers include clauses that prohibit attempts at re-identification. Audience Partners urged the Commission to ensure that these prongs strike an appropriate balance between the need for oversight to protect against privacy risks and burdens imposed on BIAS providers.

4. The Rule Should Contain an Exception to Allow Political Outreach and Other Non-Commercial Speech to Continue Unhindered.

Finally, Audience Partners urged the Commission to consider an exemption for non-commercial speech by political and non-profit organizations. Audience Partners reiterated that the Commission's Order should create an exception for non-commercial activities by political organizations and non-profits, consistent with other consumer protection regimes such as CAN-SPAM, Do-Not-Call, and the TCPA.[18] The Internet is an essential platform for political and societal discourse and the protection of First Amendment rights. Audience Partners noted the important role that tax-exempt, non-profit, and political organizations play in facilitating that dialogue. Audience Partners, agreeing with the CCA, noted in its reply comments that the Commission's proposal should clearly exempt providers when they use customer PI for non-commercial purposes or should otherwise provide an exemption for political speech and other non-commercial speech by political, non-profit, and charitable organizations.

5. Conclusion

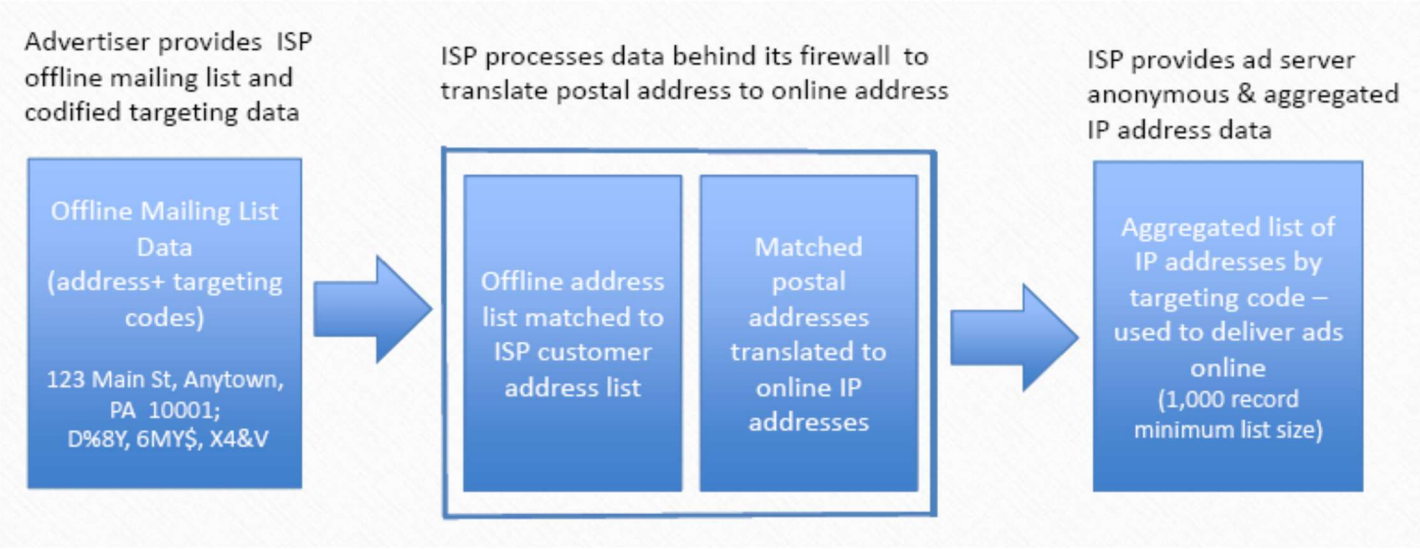
As compared to other ad serving platforms that rely on more extensive amounts of personal information and more invasive tactics, Audience Partners stressed that its technology is a viable, commercial example of how consumer information can be used to provide targeted advertising in a way that is respectful of consumers' privacy. Audience Partners encouraged the Commission to ensure that its resulting privacy regime promotes such privacy-by-design technologies and that the regime not be structured in a way that cedes online advertising to entities that use more invasive practices that are less respectful of consumer privacy. Audience Partners supports a broader, sensitivity-based opt-out framework and is willing to work with the Commission on the details of developing such a framework to promote commerce in a way that is respectful of consumer privacy.

Please direct any questions to the undersigned.

Gregory W. Guice
Jo-Ellyn Sakowitz Klein
Akin Gump Strauss Hauer and Feld LLP
1333 New Hampshire Avenue, NW
Washington, DC 20036
(202) 887-4565
Counsel for Audience Partners, LLC

[18] Audience Partners reply comments at 7-9.

Audience Partners' Doubleblind Privacy® Technique



Doubleblind Privacy® Process Description

1. Audience Partners enters into an arrangement with a BIAS provider to install a piece of hardware—a "compiler"—within the BIAS provider's network and behind its firewall.
2. An advertiser identifies an audience for a campaign and sends a mailing list and corresponding targeting code to Audience Partners (e.g., a list of addresses for households that are likely dog owners, with targeting code "LDO1"). (Either the advertiser or Audience Partners strips out all names and identifiers other than physical address from the list.)
3. Audience Partners masks the targeting code with a new random code (e.g., replacing "LDO1" with "Address List X"), in case the targeting code describes the characteristics of the audience.
4. Audience Partners sends the physical address list and masked code to the BIAS provider's compiler.
5. To complete the match, the BIAS provider provides physical address and IP address information to the compiler, and the compiler matches the data to create an aggregated list containing only IP addresses ("IP List X," comprised only of IP addresses, and including no physical address information and no other consumer data). The compiler gathers no timestamp information and has no access to the BIAS provider's active network path.

   **Note: Persistent opt-out requests from the BIAS provider's customers are implemented at the household level, so opt-outs apply even if the customer uses a different personal device or browser. The BIAS provider places an opt-out flag into the compiler along with the physical address and IP address. Addresses with an opt-out flag are ignored by the compiler in all subsequent match operations and automatically removed from any IP address lists already processed.
6. Audience Partners receives the aggregated list of IP addresses ("IP List X") and re-associates that list with the advertiser's original targeting code to allow ads to be served through an ad server to the appropriate audience.